FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, September 4, 2026

A Cyberattack Is No Longer Just An IT Problem, But a Major Financial Risk to Your Business

Source: Wipfli

For years, cybersecurity was seen as a technology issue that was owned and managed by the IT department. But in today's business landscape, that mindset is not only outdated — it's actively dangerous.

Cybersecurity-related financial risks now represent a direct threat to your company's balance sheet, valuation, business continuity and reputation. A successful cyberattack can hurt your business by impacting everything from your cash flow and insurance premiums to client retention and regulatory exposure.

If you work in finance, operations or executive leadership and still think of cyber as "IT's problem," you may be ignoring your company's biggest financial risk.

Cyber incidents are no longer rare events targeting global enterprises. Mid-market companies are squarely in the crosshairs — often because they have valuable data, financial assets and vendor relationships, but fewer security resources.

(*Click the heading link to read more.*)

Top News

How Criminals Use Title Theft to Take People's Homes

Source: IDX

Real estate fraud accounted for $275 million in losses last year

Imagine suddenly losing your home—one you might have owned and lived in for decades—including all the equity you've built up over the years and perhaps even your life's savings.

It can happen through a relatively rare phenomenon called deed fraud, also known as home title theft. The National Association of Realtors defines this scam as the illegal transfer of a property deed (a legal document outlining title ownership) without the owner's knowledge or full consent. When the scheme involves a fraudster impersonating a homeowner, it's a form of identity theft.

This type of fraud can generally be avoided by taking some basic precautions. When it does occur, however, it can be distressing for victims. According to the FBI's Internet Crime Report, the agency received more than 12,000 complaints last year regarding real estate fraud, resulting in $275 million in financial losses.

How the scam works

Fraudsters often use public records to target older homeowners—in fact, adults 50+ suffered the greatest amount of losses from real estate scams in 2025, totaling $46.4 million—or those who are at risk of foreclosure, tax judgments, utility shutoffs, or other legal or financial difficulties.

According to AmeriSave Mortgage Corporation, the types of properties most often targeted are vacant land, vacation homes, rental units, and homes with no mortgage, because scammers believe the records of these properties aren't often checked by owners.

(Click the heading link to read more.)

Microsoft Observed 7.6 Billion Phishing Emails in Q2 2026

Source: Adyen

Researchers at Microsoft warn that phishing emails are still the top initial access vector, with more than 2 billion phishing threats detected each month during the second quarter of 2026.

"Microsoft detected approximately 7.6 billion email-based phishing threats throughout the quarter, with monthly volumes declining modestly from 2.7 billion in April to 2.4 billion in June," the researchers write. "Credential phishing remained the dominant objective behind malicious payloads, while business email compromise (BEC) activity largely returned to historical norms after a brief, anomalous surge in April. Notable campaigns observed during the quarter also demonstrated how threat actors combine automation, trusted services, and multi-stage delivery chains to scale operations."

Notably, Microsoft observed a business email compromise (BEC) campaign that targeted 42,000 organizations in under three hours.

"On June 1, 2026, Microsoft Defender Research observed a high-volume BEC campaign that used automation to operate at scale," the researchers write. "Over a send window of under three hours (14:08–16:52 UTC), the actor reached more than 67,000 users across more than 42,000 organizations, almost exclusively in the United States. Targeting spanned a broad range of industries rather than a single vertical, most notably retail and consumer goods (17%), technology and software (15%), and financial services (14%). The campaign ran two...

(Click the heading link to read more.)

Continuous Identity Verification in Mobility: Why Re-verification Is Already Essential For Platform Trust

Source: Veriff

A one-time identity check tells you who someone was the day they signed up. It doesn't tell you who's behind the wheel today.

And that gap is exactly where the risk lives on mobility and delivery platforms. An account that passed onboarding can get rented out weeks later. A verified driver can get phished and lose control of their own account. Meanwhile the platform's still sitting there with a green checkmark from day one, with no way to tell the difference.

The short answer: covering this gap takes a layered system, not a single check. That means passive background monitoring of every account (device changes, location anomalies, unusual behavior), biometric re-verification triggered by those signals or run periodically as a baseline, and mandatory step-up checks locked onto high-value actions like payout changes, password resets, and account recovery.

The scale of this isn't small, either. Across the digital platforms Veriff analyzed in its Identity Fraud Report 2026, the net fraud rate hit 4.18% in 2025, roughly 1 in every 25 verification attempts, and impersonation fraud made up more than 85% of those cases. For mobility platforms running on thin margins, that's not an abstract risk; every one of those cases is a real cost, from wasted acquisition spend to the operational work of catching and removing the account.

Why is continuous identity verification a strategic priority for mobility platforms?

(Click the heading link to watch the recording.)

How CFIs Can Help Combat Elder Financial Fraud

Source: PCBB Daily Newsletter

National Senior Citizens Day fell on August 21, a time to recognize and honor the seniors in our lives. It also serves as a reminder of our responsibility to help safeguard them from financial harm. The growing threat of elder financial fraud can wipe out a lifetime of savings in a single transaction. Recent data shows that adults 60 and older now suffer the largest reported fraud losses of any age group, as criminals combine social engineering, generative AI, and crypto-enabled schemes to target older consumers at scale. This age group reported 201,266 complaints of internet-enabled fraud in 2025, with losses of approximately $7.7B, a 59% jump from 2024.

Other data sources suggest that even these alarming figures understate the problem, since many older adults never report fraud due to shame, fear of losing independence, or distrust of authorities. The Federal Trade Commission (FTC) estimates that adults 60+ reported more than $2.4B in fraud losses in 2024, with the number of older adults scammed out of $10,000 plus, more than quadrupling since 2020, while research suggests that only a fraction of incidents ever come to light.

Common Scam Tactics Used Against Older Customers

Elder-targeted financial fraud covers everything from caregivers misusing access to accounts to scammers grooming isolated individuals online or by phone. Increasingly, victims are persuaded to move money themselves, which makes it far harder for community financial institutions (CFIs) to distinguish legitimate transactions from fraud. In this environment, employee education on the most frequent scam patterns is critical.

(Click the heading link to read more.)